

MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI
FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

“AL-FARG‘ONIIY AVLODLARI”

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI



4-SON 1(4)
2023-YIL

TATU, FARG'ONA
O'ZBEKISTON



O'ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
FARG'ONA FILIALI



Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali.

Chop etish tili: O'zbek, ingliz, rus. Jurnal texnika fanlariga ixtisoslashgan bo'lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo'nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.

Язык издания: узбекский, английский, русский. Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.

Language of publication: Uzbek, English, Russian. The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2023 yil, Tom 1, №4
Vol.1, Iss.4, 2023 y

ELEKTRON ILMIY JURNALI

ELECTRONIC SCIENTIFIC JOURNAL

«Al-Farg'oniyl avlodlari» («The descendants of al-Fargani», «Potomki al-Fargani») O'zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro'yxatdan o'tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo'nalishida milliy nashrlar ro'yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg'ona sh.,
Aeroport ko'chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

Qo'lyozmalar taqrizlanmaydi va qaytarilmaydi.

FARG'ONA - 2023 YIL

TAHRIR HAY'ATI

Maxkamov Baxtiyor Shuxratovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti rektori, iqtisodiyot fanlari doktori, professor

Muxtarov Farrux Muhammadovich,

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg'ona filiali direktori, texnika fanlari doktori

Arjannikov Andrey Vasilevich,

Rossiya Federatsiyasi Sibir davlat universiteti professori, fizika-matematika fanlari doktori

Satibayev Abdugani Djunosovich,

Qirg'iziston Respublikasi, Osh texnologiyalari universiteti, fizika-matematika fanlari doktori, professor

Rasulov Akbarali Maxamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Axborot texnologiyalari kafedrasida professori, fizika-matematika fanlari doktori

Yakubov Maksadxon Sultaniyazovich,

Muhammad al-Xorazmiy nomidagi TATU «Axborot texnologiyalari» kafedrasida professori, t.f.d., professor, xalqaro axborotlashtirish fanlari Akademiyasi akademigi

G'ulomov Sherzod Rajaboyevich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent

G'aniyev Abduxalil Abdjalilovich,

Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti, Axborot xavfsizligi kafedrasida t.f.n., dotsent

Zaynidinov Hakimjon Nasritdinovich,

Muhammad al-Xorazmiy nomidagi TATU Kompyuter injiniringi fakulteti, Sun'iy intellekt kafedrasida texnika fanlari doktori, professor

Bo'taboyev Muhammadjon To'ychiyevich,

Farg'ona politexnika instituti, Iqtisod fanlari doktori, professor

Abdullayev Abdujabbor,

Andijon mashinosozlik instituti, Iqtisod fanlari doktori, professor

Qo'ldashev Abbosjon Hakimovich,

O'zbekiston milliy universiteti huzuridagi Yarimo'tkazgichlar fizikasi va mikroelektronika ilmiy-tadqiqot instituti, texnika fanlari doktori, professor

Ergashev Sirojiddin Fayazovich,

Farg'ona politexnika instituti, elektronika va asbobsozlik kafedrasida professori, texnika fanlari doktori, professor

Qoraboyev Muhammadjon Qoraboevich,

Toshkent tibbiyot akademiyasi Farg'ona filiali fizika matematika fanlari doktori, professor, BMT ning maslahatchisi maqomidagi xalqaro axborotlashtirish akademiyasi akademigi

Polvonov Baxtiyor Zaylobiddinovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy ishlar va innovatsiyalar bo'yicha direktor o'rinbosari

Zulunov Ravshanbek Mamatovich,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Dasturiy injiniring kafedrasida dotsenti, fizika-matematika fanlari nomzodi

Saliyev Nabijon,

O'zbekiston jismoniy tarbiya va sport universiteti Farg'ona filiali dotsenti

Abdullaev Temurbek Marufovich,

Muhammad al-Xorazmiy nomidagi TATU Axborot texnologiyalari kafedra mudiri, texnika fanlar bo'yicha falsafa doktori

Zokirov Sanjar Ikromjon o'g'li,

Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i, fizika-matematika fanlari bo'yicha falsafa doktori

Jurnal quyidagi bazalarda indekslanadi:



Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Muxtarov Farrux Muhammadovich, TARMOQ TRAFIGI ANOMALIYALARINI IDENTIFIKATSIYA QILISHNING STATIK USULI	4-7
Daliyev Baxtiyor Sirojiddinovich, Abelning umumlashgan integral tenglamasini yechish uchun Sobolev fazosida optimal kvadratur formulalar	8-14
Umarov Shuxratjon Azizjonovich, KRIPTOBARDOSHLI KRIPTOGRAFIK TIZIMLAR VA ULARNING KLASSIFIKATSIYASI	15-21
Zulunov Ravshanbek Mamatovich, PYTHONDA NEYRON TARMOQNI QURISH VA BASHORAT QILISH	22-26
Djalilov Mamatisa Latibdjanovich, IKKI QATLAMLI NOELASTIK PLASTINKANING KO'NDALANG TEBRANISHI UMUMIY TENGLAMASINI TAHLIL QILISH	27-30
Erkin Uljaev, Azizjon Abdulkhamidov, Utkirjon Ubaydullayev, A Convolutional Neural Network For Classification Cotton Boll Opening Degree	31-36
Seytov Aybek Jumabayevich, Xusanov Azimjon Mamadaliyevich, Magistral kanallarda suv resurslarini boshqarish jarayonlarini modellashtirish algoritmini ishlab chiqish	37-43
Abdullayev Temurbek Marufjonovich, Algorithm of functioning of intellectual information-measuring system	44-49
Odinakhon Sadikovna Rayimjanova, Usmonali Umarovich Iskandarov, Reaserch of highly sensitive deformation semiconductor sensors based on AFV	50-53
S.S.Radjabov, G.R.Mirzayeva, A.O.Tillavoldiyev, J.A.Allayorov, BARG TASVIRI BO'YICHA MADANIY O'SIMLIK LARNING FITOSANITAR HOLATINI ANIQLASH ALGORITMLARI	54-59
Эргашев Отабек Мирзапулатович, Интеллектуальный оптоэлектронный прибор для учета и контроля расходом воды в открытых каналах	60-65
Xomidov Xushnudbek Rapiqjon o'g'li, Nurmatov Sardorbek Xasanboy o'g'li, Yo'ldashev Bilol Iqboljon o'g'li, O'lmasov Farrux Yorqinjon o'g'li, Konus setkali chang tozalovchi qurilma uchun chang namunalarning dispers tarkibi tahlili	66-69
Akhundjanov Umidjon Yunus ugli, VERIFICATION OF STATIC SIGNATURE USING CONVOLUTIONAL NEURAL NETWORK	70-74
Лазарева Марина Викторовна, Горовик Александр Альфредович, Цифровизация и цифровой менеджмент в современном управлении	75-81
D.X.Tojimatov, KIBERTAHDIDLARNI OLDINI OLIHDA KIBERRAZVEDKA AMALIYOTI VA UNING USTUVOR VAZIFALARI	82-85
Muxtarov Farrux Muhammadovich, Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, Kompyuter eksperimenti orqali kam atomli mis klasterlarining geometrik tuzilishini o'rganish	86-89
Umurzakova Dilnoza Maxamadjanovna, BOSHQARISH QONUNLARINI ADAPTATSIYALASH ALGORITMLARINI ISHLAB CHIQLASH	90-94
Muxamedieva Dildora Kabilovna, Muxtarov Farrux Muhammadovich, Sotvoldiev Dilshodbek Marifjonovich, JAMOAT TRANSPORTI MARSHRUTLARINI QURISH INTELLEKTUAL ALGORITMLARI	95-103
Нурдинова Разияхон Абдихаликовна, Перспективы применения элементов с аномальными фотовольтаическими напряжениями	104-108
Bozarov Baxromjon Pخomovich, UCH O'LCHOVLI FAZODAGI SFERADAANIQLANGAN FUNKSIYALARNI TAQRIBIY INTEGRALLASH UCHUN OPTIMAL KUBATUR FORMULALAR	109-113
Улжаев Эркин, Худойбердиев Элёр Фахриддин угли, Нарзуллаев Шохрух Нурали угли, РАЗРАБОТКА КОНСТРУКЦИИ И ФУНКЦИОНАЛЬНОЙ СХЕМЫ ПОЛУЦИЛИНДРИЧЕСКОГО ЁМКОСТНОГО ПОТОЧНОГО ВЛАГОМЕРА	114-122
Mamirov Uktam Farkhodovich, Buronov Bunyod Mamurjon ugli, ALGORITHMS FOR FORMATION OF CONTROL EFFECTS IN CONDITIONS OF UNOBSERVABLE DISTURBANCES	123-127
Sharibayev Nosirjon Yusubjanovich, Jabborov Anvar Mansurjonovich, YURAK-QON TOMIR KASALLIKLARI DIAGNOSTIKASI UCHUN TEXNOLOGIYALAR, ALGORITMLAR VA VOSITALAR	128-136
Marina Lazareva, Estimating development time and complexity of programs	137-141
Asrayev Muhammadmullo, ONLINE HANDWRITING RECOGNITION	142-146
Norinov Muhammadyunus Usibjonovich, SPEKTR ZONALI TASVIRLARGA INTELLEKTUAL ISHLOV BERISH USULLARI TAHLILI	147-152
Xudoynazarov Umidjon Umarjon o'g'li, PARAMETRLI ALGEBRAGA ASOSLANGAN EL-GAMAL SHIFRLASH ALGORITMLARINI GOMOMORFIK XUSUSIYATINI TADQIQ ETISH	153-157
D.M.Okhunov, M.Okhunov, THE ERA OF THE DIGITAL ECONOMY IS AN ERA OF NEW OPPORTUNITIES AND PROSPECTS FOR BUSINESS DEVELOPMENT BASED ON CROWDSOURCING TECHNOLOGIES	158-165

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Солиев Бахромжон Набиджонович, Путеводитель по построению веб-API на Django - Шаг за шагом с Django REST framework — от моделей до проверки работоспособности	166-171
Sevinov Jasur Usmonovich, Boborayimov Okhunjon Khushmurod ogli, ALGORITHMS FOR SYNTHESIS OF ADAPTIVE CONTROL SYSTEMS WITH IMPLICIT REFERENCE MODELS BASED ON THE SPEED GRADIENT METHOD	172-176
Mamatov Narzullo Solidjonovich, Jalelova Malika Moyatdin qizi, Tojiboyeva Shaxzoda Xoldorjon qizi, Samijonov Boymirzo Narzullo o'g'li, SUN'IY YO'LDOSHDAN OLINGAN TASVIRDAGI DALA MAYDONI CHEGARALARINI ANIQLASH USULLARI	177-181
Обухов Вадим Анатольевич, Криптография на основе эллиптических кривых (ECC)	182-188
Turdimatov Mamirjon Mirzayevich, Sadirova Xursanoy Xusanboy qizi, AXBOROTNI HIMOYALASHDA CHETLAB O'TISHNING MUMKIN BO'LGAN EHTIMOLLIK XOLATINI BAHOLASH USULLARI	189-193
Musayev Xurshid Sharifjonovich, TRIKOTAJ MAHSULOTLARIDA NUQSONLI TO'QIMALARNING ANIQLASHNING MATEMATIK MODELI VA UNING ALGORITMLARI	194-196
Kodirov Ahkhmadkhon, Umarov Abdumukhtar, Rozaliyev Abdumalikjon, ANALYSIS OF FACIAL RECOGNITION ALGORITHMS IN THE PYTHON PROGRAMMING LANGUAGE	197-205
Suyumov Jorabek Yunusalievich, METHODOLOGICAL PROBLEMS OF QUALIMETRY IN CONDUCT OF PEDAGOGICAL EXPERIMENT-EXAMINATION	206-211
Хаджаев Саидакбар Исмоил угли, АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ МАЛОГО И СРЕДНЕГО БИЗНЕСА ОТ КИБЕРАТАК	212-217
M.M.Khalilov, Effect of Heat Treatment on the Photosensitivity of Polycrystalline PbTe Films AND PbS	218-221
Тажибаев Илхом Бахтиёрвич, ПОЛНОСТЬЮ ВОЛОКОННЫЙ СЕНСОР, ОСНОВАННЫЙ НА КОНСТРУКЦИИ ИЗ МАЛОМОДОВОГО ВОЛОКОННОГО СМЕЩЕНИЯ С КАСКАДНЫМ СОЕДИНЕНИЕМ ВОЛОКОННОЙ РЕШЕТКИ С БОЛЬШИМ ИНТЕРВАЛОМ, ИСПОЛЬЗУЕТСЯ ДЛЯ ОПРЕДЕЛЕНИЯ ИСКРИВЛЕНИЯ И ПРОВЕДЕНИЯ АКУСТИЧЕСКИХ ИЗМЕРЕНИЙ	222-225
Sharibaev Nosir Yusubjanovich, Djuraev Sherzod Sobirjanovich, To'xtasinov Davronbek Xoshimjon o'g'li, PRIORITIES IN DETERMINING ELECTRIC MOTOR VIBRATION WITH ADXL345 ACCELEROMETER SENSOR	226-230
Mukhammadjonov A.G., ANALYSIS OF AUTOMATION THROUGH SENSORS OF HEAT AND HUMIDITY OF DIFFERENT DIRECTIONS	231-236
Эрматова Зарина Кахрамоновна, АКТУАЛЬНОСТЬ ПРЕПОДАВАНИЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ C++ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ	237-241
Saparbaev Rakhmon, ANALOG TO DIGITAL CONVERSION PROCESS BY MATLAB SIMULINK	242-245
Садикова М.А., Авазова Н.К., САМООБУЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, БАЗОВЫЕ ПРИНЦИПЫ РАБОТЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ПРОСТОМ ПРИМЕРЕ	246-250
Abduhafizov Tohirjon Ubaydullo o'g'li, Abdurasulova Dilnoza Botirali kizi, DEVELOPMENT OF ALGORITHMS IN THE ANALYSIS OF DEMAND AND SUPPLY PROCESSES IN ECONOMIC SYSTEMS	251-256
Kayumov Ahror Muminjonovich, CREATING MATHEMATICAL MODELS TO IDENTIFY DEFECTS IN TEXTILE MACHINERY FABRIC	257-261
Mirzakarimov Baxtiyor Abdusalomovich, Xayitov Azizjon Mo'minjon o'g'li, BIOMETRIC METHODS SECURE COMPUTER DATA FROM UNAUTHORIZED ACCESS	262-266
Soliyev B., Odilov A., Abdurasulova Sh., Leveraging Python for Enhanced Excel Functionality: A Practical Exploration	267-271
Жураев Нурмахамад Маматович, Системы Электроснабжения Оборудования Предприятий Связи: Надежность и Эффективность	272-276
Rasulova Feruzaxon Xoshimjon qizi, Isroilov Sharobiddin Mahammadyusufovich, OLIY TA'LIM MUASSASALARIDA MUTAXASSISILIK FANLARINI O'QITISHDA MULTIMEDIALI MOBIL ILOVADANDAN FOYDALANISHNING STATISTIK TAHLILI	277-280
Muxtarov Farrux Muxammadovich, Toshpulatov Sherali Muxamadaliyevich, SUN'IY INTELLEKT YORDAMIDA IJTIMOYIY TARMOQ MONITORINGI TIZIMINI YARATISH, AFZALLIKLARI VA MUHIM JIXATLARI	281-285
Sadikova Munira Alisherovna, APPLICATION OF ARTIFICIAL INTELLIGENCE DEVICES IN MANUFACTURING	286-290
Mamatov Narzullo Solidjonovich, Ibroximov Sanjar Rustam o'g'li, Fayziyev Voxid Orzumurod o'g'li, Samijonov Abdurashid Narzullo o'g'li, SUN'IY INTELLEKT VOSITALARINI TA'LIMNI NAZORAT QILISH VA BAHOLASHDA QO'LLASH	291-297

Криптография на основе эллиптических кривых (ECC)

Обухов Вадим Анатольевич,

ассистент кафедры «Информационные технологии»

Ферганского филиала

Ташкентского университета информационных

технологий имени Мухаммада Ал-Хорезми,

e-mail: wendigo_chelsea@mail.ru

Аннотация. Криптография с эллиптической кривой (ECC), как одна из наиболее важных современных криптографий, более надежна, чем большинство других криптографий, как с точки зрения безопасности, так и с точки зрения надежности, поскольку она использует эллиптическую кривую для построения и в то же время использует математические операции для шифрования и генерации ключей. В то же время криптография на основе эллиптических кривых может продолжать улучшать скорость и интенсивность за счет совершенствования ускорителей, скалярного умножения и скорости обработки ордеров.

Ключевые слова: криптография на основе эллиптических кривых (ECC); криптография; код RSA; алгоритм цифровой подписи на основе эллиптических кривых (ECDSA).

Введение. Криптография – это искусство тайной передачи информации. Сегодня людям нужна криптография, чтобы побеждать в войнах, строить Интернет и так далее. Криптография является важным инструментом для развития человеческого общества.

В этой статье мы суммировали введение в криптографию, введение в эллиптические кривые, принцип работы ECC, сравнение ECC с другими кодами, прорыв в ECC и применение ECC, используя метод обзора литературы [1].

Был представлен обзор развития ECC. Сравнение может прояснить преимущества и недостатки ECC. Чтобы внести некоторые прямые улучшения, введение в эллиптические кривые и принципы работы ECC может рассказать общественности об ECC; введение в криптографию может повысить осведомленность общественности о криптографии; а применение ECC может помочь людям узнать, как ECC действительно помогает им в повседневной жизни. Прежде всего, эта статья помогает большему количеству людей узнать о криптографии, особенно ECC, и о том, как вместе внести некоторые улучшения в будущее. Кроме того, в этой статье приводятся некоторые практические пути и направления улучшения ECC, давая краткое изложение того, что люди делали для его улучшения раньше.

Литературный обзор и методология.

Криптография – это искусство сокрытия информации. Люди используют криптографию для передачи информации.

Криптография имеет долгую историю; она была открыта около 400 лет назад. До 1949 года люди использовали классические коды. Классические коды имеют низкую интенсивность, а значит, их легко взломать. Между 1950 и 1975 годами криптография постепенно проникла в сознание людей и стала наукой. С 1976 года по настоящее время ключ в криптографии добился большого прогресса. С этого момента криптография начала делиться на несколько ветвей.

Классификация криптографии.

После того, как криптография начала иметь ответвления, криптография была разделена на симметричную и асимметричную криптографию (криптографию с открытым ключом). Среди них криптография с открытым ключом является основным направлением изучения криптографии, а также самой невзламываемой криптографией.

Криптография с открытым ключом.

Криптография RSA и криптография на основе эллиптических кривых (ECC) являются двумя основными кодами криптографии с открытым ключом.



Криптография с открытым ключом в основном использует математические вычисления для шифрования и дешифрования. Например, криптография RSA использует огромное число, которое трудно разделить на два больших простых числа, чтобы сделать код более надежным [2].

Криптография с открытым ключом более современна, чем традиционная криптография, и ее безопасность выше, чем у традиционной криптографии, поскольку длина ее ключа больше, а для ее расшифровки требуется больше вычислений. Однако криптография с открытым ключом не заменит полностью традиционную криптографию, поскольку требует большого количества вычислений, поэтому ее можно использовать только для подписей и управления ключами.

	Традиционная криптография	Криптография с открытым ключом
Базовые требования	1. Отправители и получатели должны использовать общий ключ.	1. Отправитель владеет одним ключом шифрования или дешифрования, а получатель — другим.
	2. Отправители и получатели должны использовать один и тот же ключ и один и тот же алгоритм.	2. При шифровании и дешифровании используется один и тот же алгоритм, но разные ключи.
Требования безопасности	1. Не зная ключа, невозможно расшифровать	1. Не зная ключа, невозможно расшифровать
	2. Если известен только алгоритм и несколько зашифрованных текстов, подтвердить ключ невозможно.	2. Если известен только один ключ и несколько зашифрованных текстов, невозможно подтвердить другой ключ.
	3. Ключ следует хранить в тайне.	3. Закрытый ключ должен храниться в тайне.

Таблица 1 (Table 1). Сравнение традиционной криптографии и криптографии с открытым ключом.

Эллиптические кривые.

Криптография с эллиптической кривой — важный тип шифрования в криптографии с открытым ключом, который использует эллиптическую кривую для шифрования и дешифрования.

Эллиптическая кривая — это гладкая аффинная кривая с родом 1 в области определения, и ее выражение можно записать как $y^2 = x(x-1)(x-\lambda)$, $\lambda \neq 0,1$, или $y^2 + ay = x^3 + bx^2 + cx + d$. Если характеристики области не 2 и 3, то ее также можно записать как $y^2 = x^3 + ax + b$.

Графики эллиптических кривых изменяются в зависимости от их коэффициентов, как показано на графиках ниже [3].

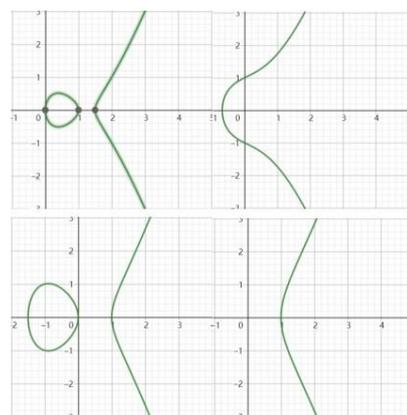


Рисунок 1 (Picture 1). Четыре разные эллиптические кривые.

Эллиптические кривые имеют несколько приложений, таких как криптография эллиптических кривых (ECC), алгоритм цифровой подписи эллиптических кривых (ECDSA) и т. д.

Чтобы понять криптографию эллиптических кривых, нам также необходимо знать определение группы.

Если непустая группа G определена как имеющая операцию « \cdot », и эта операция выполняется:

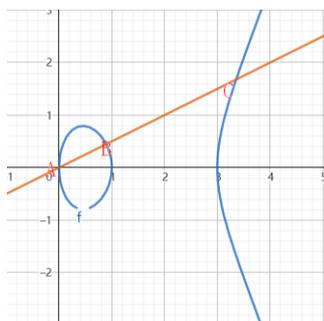
- $\forall x, y \in G$, удовлетворяют значению $x \cdot y \in G$
- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\forall x \in G$, $\exists p$, так как $p \cdot x = x$
- $\forall x \in G$, $\exists y$, так как $x \cdot y = y \cdot x = q$



тогда мы можем сказать, что G — группа относительно операции « \cdot ». Если G также удовлетворяет коммутативной аксиоме, то G — Абелева группа.

Аддитивная группа на эллиптических кривых.

На эллиптической кривой нам нужно определить «аддитивную группу» для последующих криптографических вычислений.



$$(P + xA) - kxB$$

Рисунок 2 (Picture 2). Четыре разные эллиптические кривые.

На эллиптической кривой мы случайным образом выбираем две точки A и B . Затем проводим линию AB и пересекаем эллиптическую кривую в точке C . Затем определяем $A+B+C$.

Если A и B — одни и те же точки, то C — точка пересечения касательной линии A и эллиптической кривой [4].

Доказано, что аддитивная группа эллиптической кривой соответствует требованиям группы, поэтому она является группой, а также соответствует коммутативной аксиоме, поэтому она является абелевой группой.

Порядок эллиптических кривых.

Порядок эллиптической кривой также является важным базовым знанием эллиптической кривой.

Если эллиптическая кривая существует в конечных полях, порядок существует. Порядок — это количество точек в ограниченной области эллиптической кривой.

Основной принцип криптографии с эллиптическими кривыми (ECC).

Составляющая криптографии с эллиптическими кривыми (ECC).

Кодовая система состоит из открытого текста, ключа и зашифрованного текста, причем ключ может быть открытым, закрытым или частично открытым и частично закрытым.

Формирование ключа криптографии с эллиптическими кривыми (ECC).

Автор случайным образом выбирает две точки A и B на эллиптической кривой, B является кардинальной точкой эллиптической кривой, а A удовлетворяет условию $A = kB$. Затем задается для закрытого ключа значение k , а для открытого ключа — A . Используя аддитивную группу на эллиптической кривой, если мы знаем только k и B , легко найти A , но если мы знаем только A и B , трудно найти k [5].

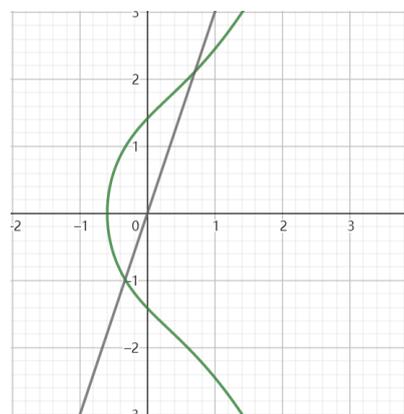


Рисунок 3 (Picture 3). Линия, проходящая через эллиптическую кривую.

Шифрование криптографии с эллиптическими кривыми (ECC).

Во-первых, кодировщик должен посредством некоторых изменений преобразовать предложения в открытом тексте в несколько чисел.

Затем кодер должен случайным образом найти конкретную эллиптическую кривую.

Установите открытый текст как P , выберите число x ($x < n$, n — порядок конкретной эллиптической кривой) случайным образом.

Посредством преобразования $Q = (xB, P + xA)$ кодер преобразует открытый текст P в зашифрованный текст Q . Сложение в этом преобразовании является обычным алгебраическим сложением. Затем



измените зашифрованный текст Q на слова, внося некоторые изменения [6].

Расшифровка криптографии с эллиптическими кривыми.

Декодер получит закрытый ключ k , поэтому декодер может использовать уравнение для поиска открытого текста P , потому что $(P + xA) - kxB = P + kxB - kxB = P$.

Причина, по которой ECC использует эллиптические кривые.

- 1) Линия, проходящая через случайную точку эллиптической кривой, скорее всего, будет иметь три точки пересечения со всей эллиптической кривой. Это удовлетворяет требованиям добавки к эллиптическим кривым, которые требует ECC.
- 2) Существует несколько форм эллиптических кривых. Изменение коэффициента может привести к изменению формы всей эллиптической кривой.

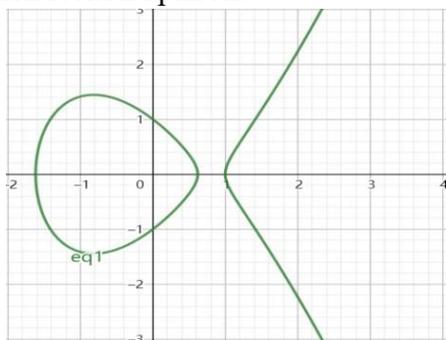


Рисунок 4 (Picture 4). $y^2 = x^3 - 2x + 1$

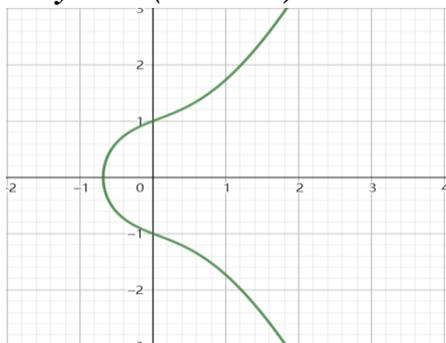


Рисунок 5 (Picture 5). $y^2 = x^3 + x + 1$

Это удовлетворяет требованию разнообразия эллиптических кривых в ECC.

Сравнение криптографии ECC и RSA

Сравнение ключевых моментов криптографии ECC и RSA.

Ключом к криптографии RSA является то, что большое число, умноженное на два больших простых числа, является открытым ключом и его трудно разобрать. Однако эффективность генерации двух огромных простых чисел ниже, чем у криптографии на эллиптических кривых [7].

Криптография с эллиптической кривой (ECC) использует обратную операцию сложения эллиптической кривой в качестве ключа и позволяет добиться высокого уровня шифрования без сложных операций, поэтому ее эффективность относительно выше. Кроме того, до сих пор не было обнаружено каких-либо очевидных уязвимостей ECC, поэтому это относительно надежная современная криптография.

Анализ преимуществ криптографии на основе эллиптических кривых (ECC).

Во-первых, криптография на основе эллиптических кривых имеет более высокий уровень безопасности. Система шифрования с эллиптической кривой обеспечивает более надежную защиту и лучше, чем любой другой алгоритм шифрования, предотвращает атаки, делает веб-сайты и инфраструктуру более безопасными, чем традиционные методы шифрования, что позволяет ECC обеспечить лучшую гарантию безопасности мобильного Интернета [8].

Во-вторых, криптография на основе эллиптических кривых лучше подходит для мобильного Интернета. Криптография с эллиптической кривой имеет относительно короткий ключ длиной 256 бит, поэтому она занимает меньше места для хранения. Поскольку все больше и больше пользователей используют мобильные устройства для выполнения различных действий в Интернете, криптография на основе эллиптических кривых обеспечивает лучшее качество обслуживания клиентов в области безопасности мобильного Интернета.

В-третьих, криптография на основе эллиптических кривых имеет лучшие свойства. Криптография на основе эллиптических кривых



может обеспечить лучшую безопасность при более коротких длинах ключей. Например, стойкость ключа 256-битной криптографии с эллиптической кривой примерно такая же, как и стойкость 3072-битного ключа RSA (в настоящее время нормальная длина ключа RSA составляет 2048 бит). Согласно тестам соответствующих зарубежных органов, время отклика веб-сервера более чем в десять раз быстрее, чем у RSA при использовании алгоритма ECC на серверах Apache и IIS.

Анализ недостатков криптографии на основе эллиптических кривых (ECC).

Основным недостатком криптографии на основе эллиптических кривых является ее низкая эффективность. Эллиптическая криптография опирается на математические вычисления для шифрования и дешифрования, а ее надежность зависит от сложности вычислений. Поэтому его расчет огромен, что приводит к низкой эффективности передачи, шифрования и дешифрования [9].

Результаты.

Улучшения Ускорителя.

Одним из основных недостатков криптографии с открытым ключом является то, что она требует слишком много вычислений и потребляет слишком много энергии и времени, поэтому улучшение ускорителя крайне необходимо для повышения эффективности шифрования и дешифрования эллиптических кривых, а также генерации ключей. Нынешние отечественные и зарубежные студенты университетов, имеющие большой опыт в криптографии на эллиптических кривых, стремятся исследовать способы повышения эффективности и постепенно находят более подходящий ускоритель для криптографии на эллиптических кривых. Например, метод ASIC можно использовать для проектирования и реализации аппаратных ускорителей.

Ускорение алгоритма скалярного умножения.

Скорость алгоритма скалярного умножения очень важна для шифрования эллиптической криптографии. Есть два фактора, которые ускоряют алгоритм скалярного умножения: координатное представление и представление цепочки экспоненциального сложения. Представление обратных координат позволяет избежать обратной операции в конечной области. Цепочка экспоненциального сложения может обеспечить скалярное умножение с как можно меньшим количеством групп эллиптических кривых.

В настоящее время самым современным стандартом является координатное представление: нечетные объекты используют координаты Якоби, а четные — координаты LD. Повышенная скорость алгоритма скалярного умножения может с замечательным эффектом применяться к популярному оборудованию.

Улучшения порядка расчета.

Используя метод комплексного умножения, можно легко найти эллиптическую кривую, но для дальнейшего усиления безопасности системы паролей в криптографии эллиптическая кривая имеет тенденцию генерироваться случайным образом. Но эллиптические кривые, необходимые для криптографии эллиптических кривых, должны иметь один и тот же порядок, поэтому поляризация порядка становится важным эффектом при создании эллиптических кривых.

В 1984 году Шуф с помощью алгоритма с полиномиальным временем предложил вычислить порядок метода эллиптических кривых, но фактическая производительность алгоритма очень низкая, поэтому автор не может получить практического применения в криптографии на эллиптических кривых. Затем Элки выдвинул простые числа Элки и простые числа Аткинса, которые в конечном поле имеют более широкий контекст, предложен алгоритм и значительно повышает эффективность расчета порядка эллиптических кривых. Точно так же Лесье предложил метод использования формы способа расчета эффекта, который дал аналогичные результаты. Затем Сато и Харли предложили более



эффективный алгоритм, а также предложили такой же простой и эффективный метод расчета, позволяющий вычислить более выдающийся эффект. На данный момент эта проблема решена почти идеально несколькими криптографами и математиками [10].

Алгоритм цифровой подписи на основе эллиптических кривых (ECDSA).

Цифровая подпись не относится к реальной подписи, но закрытый ключ «подписывает» определенную информацию. Другие люди (включая пользователя B) могут проверить, что информация действительно подписана пользователем A с помощью открытого ключа пользователя A , поскольку информация может быть подписана только закрытым ключом пользователя A . Однако цифровые подписи могут использоваться для реальных подписей.

Оператор будет использовать хэш-функцию, которая находится на уровне безопасности, для преобразования открытого текста подписи P в зашифрованный текст Q . Затем оператор случайным образом генерирует другое число k ($0 < k < n$), n - это порядок циклической подгруппы. $A = kB$, определение A , B , k такое же, как и приведенное выше. Затем определяется X_p как координата X точки P , $r = x_p \bmod n$, $s = (z + rd_A) / k \bmod n$. (r, s) — это информация о подписи.

Алгоритм SM2.

SM2 имеет преимущества перед RSA с точки зрения безопасности и свойств. Таким образом, SM2 может заменить RSA. Алгоритм SM2 имеет множество применений, например, усиление информационной безопасности.

Существует связь между алгоритмом SM2 и криптографией эллиптических кривых (ECC). Алгоритм SM2 определяет свою кривую путем определения in . Кроме того, чтобы сопоставить кривые с алгоритмами шифрования, в стандарте SM2 идентифицируются другие параметры для использования алгоритмическими программами [11].

Заключение. Прежде всего, криптография быстро развивалась с древних времен. Переход от классической криптографии к современной криптографии произошел благодаря эллиптической кривой. Во-вторых, она более надежна, чем большинство других криптографий, как с точки зрения безопасности, так и с точки зрения надежности, поскольку для построения она использует эллиптические кривые и в то же время использует математические операции для шифрования и генерации ключей.

Во-вторых, криптография на основе эллиптических кривых может продолжать улучшать скорость и интенсивность за счет улучшения ускорителей, скалярного умножения и скорости обработки ордеров.

Наконец, применение эллиптической кривой в цифровой подписи в Интернете и SM2 очень эффективно, что еще раз иллюстрирует важность криптографии с эллиптической кривой.

Список литературы (References):

- Бессалов, А. В. (2017). Эллиптические кривые в форме Эдвардса и криптография.
- Болотов, А. А., Гашков, С. Б., Фролов, А. Б., & Часовских, А. А. (2006). Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. Изд. 2.
- Бессалов, А. В., Дихтенко, А. А., & Третьяков, Д. Б. (2011). Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем. Сучасний захист інформації, (4), 33-36.
- Долгов, В. И. (2008). Эллиптические кривые в криптографии. Системы обробки інформації, (6), 2-10.
- Жданов, О. Н., & Чалкин, В. А. (2013). Эллиптические кривые: Основы теории и криптографические приложения. М.: Книжный дом «ЛИБРОКОМ», 2013. 200 с.
- Левин, В. Ю. (2007). Кодирование алфавитов точками эллиптических кривых. Интеллектуальные системы, 11(1-4), 171-184.
- Марчук, К. С., & Асмыкович, И. (2019). Алгоритм создания электронной подписи на основе групп точек на эллиптической кривой. In МОЛОДЕЖЬ И



НАУКА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ
ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ. (pp. 370-373).

8. Обухов, В., Эльнур, Х., & Набижонов, Р. (2023). ПОЭТАПНОЕ ВНЕДРЕНИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН. Research and implementation.
9. Обухов, В., Ходжиматов, Ж., & Набижонов, Р. (2023). РАЗВИТИЕ БЛОКЧЕЙН ТЕХНОЛОГИЙ В УЗБЕКИСТАНЕ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ПЕРСПЕКТИВЫ. Research and implementation.
10. Обухов, В. А. (2023). Цифровая безопасность данных в блокчейн-сетях. PEDAGOG, 6(10), 304-308.
11. Обухов, В. А., & Хакимов, А. А. (2022). ОСНОВЫ ИСПОЛЬЗОВАНИЯ РЕКУРСИВНЫХ ФУНКЦИЙ В СТРУКТУРАХ ДАННЫХ. Journal of new century innovations, 11(1), 92-99.

